SACM
Internet-Draft
Intended status: Standards Track
Expires: August 3, 2018

D. Haynes
The MITRE Corporation
J. Fitzgerald-McKay
Department of Defense
L. Lorenzin
Pulse Secure
January 30, 2018

Endpoint Compliance Profile
draft-ietf-sacm-ecp-01

Abstract

This document specifies the Endpoint Compliance Profile, a high-level specification that describes a specific combination and application of IETF and TNC protocols and interfaces specifically designed to support ongoing assessment of endpoint posture and the controlled exposure of collected posture information to appropriate security applications. This document is an extension of the Trusted Computing Group's Endpoint Compliance Profile Version 1.0 specification.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 3, 2018.

Copyright Notice

Table of Contents

1. Introduction

The Endpoint Compliance Profile (ECP) builds on prior work from the IETF NEA WG, the IETF NETMOD WG, and the Trusted Computing Group [TNC]Trusted Network Communications (TNC) WG to standardize the collection, storage and sharing of posture information from network-connected endpoints, including user endpoints, servers, and infrastructure. The first generation of this specification focuses on reducing the security exposure of a network by enabling event-driven posture collection, as well as standardized querying for additional endpoint data as needed. Standardized collection improves network security by confirming that endpoints are known and authorized, and are compliant with network policy.

When ECP is used, posture collectors running on the target endpoint gather posture information as changes occur on the endpoint, and forward this information to a posture manager, which stores it in a repository. This information is gathered while the target endpoint is already connected to the network. Administrators will query the repository to determine the posture status of an endpoint.

Building and maintaining a continuously updated repository of information using the ECP enables network owners and administrators to perform the asset, vulnerability, and configuration management tasks that are the basis for robust network security.

The ECP also describes how to expose information--such as endpoint purpose, the software that is supposed to be running on an endpoint, and the activities an endpoint is supposed to be performing--to sensors that are looking for indicators of attacks and malicious activity on the network. The ECP does not set requirements for this future-leaning work; it instead sets requirements for building a data repository that best enhances decision-making by these sensors. Therefore, while data sharing components are included in ECP diagrams and high-level capability descriptions, vendors are free to experiment with best approaches for sharing data beyond the repository. Suggestions and ideas for future integration are captured in the Section 12 section of this document.

1.1. Preventative Posture Assessments

The value of continuous endpoint posture assessment is well established. Security experts have for years identified asset management and vulnerability remediation as a critical step for preventing intrusions. Application whitelisting, patching applications and operating systems, and using the latest versions of applications top the Defense Signals Directorate’s "Top 4 Mitigations to Protect Your ICT System". [DSD] "Inventory of Authorized and

Unauthorized Endpoints", "Inventory of Authorized and Unauthorized Software", and "Continuous Vulnerability Assessment and Remediation" are Critical Controls 1, 2, and 4, respectively, of the CIS "20 Critical Security Controls". [CIS] While there are commercially available solutions that attempt to address these security controls, these solutions do not run on all types of endpoints; consistently interoperate with other tools that could make use of the data collected; collect posture information from all types of endpoints in a consistent, standardized schema; or require vetted, standardized protocols that have been evaluated by the international community for cryptographic soundness.

As is true of most solutions offered today, the solution found in the ECP does not attempt to solve the lying endpoint problem. An endpoint that has already been infected with malicious software can provide false information about its identity and the software it is running. The primary purpose of the ECP is not to detect infected endpoints; rather, it focuses on ensuring that healthy endpoints remain healthy by keeping software up-to-date and patched. The first goal of the ECP is to help an administrator easily determine which endpoints require some follow-up action. By sharing posture information with sensors on the network, ECP aids in the detection of attacks on endpoints and drives follow-up actions.

1.2. All Network-Connected Endpoints are Endpoints

As defined by [I-D.ietf-sacm-terminology], an endpoint is any physical or virtual computing endpoint that can be connected to a network. Posture assessment against policy is equally, if not more, important for continuously connected endpoints, such as enterprise workstations and infrastructure endpoints, as it is for sporadically connected endpoints. Continuously connected endpoints are just as likely to fall out of compliance with policy, and a standardized posture assessment method is necessary to ensure they can be properly handled.

1.3. All Endpoints on the Network Must be Uniquely Identified

Many administrators struggle to identify what endpoints are connected to the network at any given time. By requiring a standardized method of endpoint identity, the Endpoint Compliance Profile will enable administrators to answer the basic question, "What is on my network?" Unique endpoint identification also enables the comparison of current and past endpoint posture assessments, by allowing administrators to correlate assessments from the same endpoint. This makes it easier to flag suspicious changes in endpoint posture for manual or automatic review, and helps to swiftly identify malicious changes to endpoint applications.

1.4. Standardized Data Models

The ECP requires the use of standardized data models for the exchange of posture information. This helps to ensure that the posture information sent from endpoints to the repository can be easily stored, due to their known format, and shared with authorized endpoints and users. Standardized data models also enable collection from myriad types of endpoints. Such standardization saves vendors time and money--time that does not have to be spent integrating new data models into the enterprise's reporting mechanisms, and money that does not have to be spent on developing tools to parse information from each type of endpoint connected to the network. Standardized data models also enable the development of standardized client software. This allows endpoint vendors to include their own client software that can interoperate with posture assessment infrastructure and thus not have to introduce third party code in their products.

1.5. Secure Standardized Protocols

Posture information must be sent over mature, standardized protocols to ensure the confidentiality and authenticity of this data while in transit. Conformant implementations of the ECP include [RFC6876] and [I-D.ietf-netconf-yang-push] for communication between the target endpoint and the posture manager. These protocols allow networks that implement this solution to collect large amounts of posture information from an endpoint to make decisions about that endpoint's compliance with some policy. The ECP offers a solution for all endpoints already connected to the network. Periodic assessments and automated reporting of changes to endpoint posture allow for instantaneous identification of connected endpoints that are no longer compliant to some policy.

1.6. Posture Information Must Be Stored

Posture information must be stored by the repository and must be exposed to an interface at the posture manager. Standard data models enable standard queries from an interface exposed to an administrator at the posture manager console. A repository must retain any current posture information retrieved from the target endpoint and store it indexed by the unique identifier for the endpoint. Any posture validator specified by this profile must be able to ascertain from its corresponding posture collector whether the posture information is up to date. An interface on the posture manager must support a request to the posture validator to obtain up-to-date information when an endpoint is connected. This interface must also support the ability to make a standard set of queries about the posture information stored by the repository. In the future, some forms of

posture information might be retained at the endpoint. The interface on the server must accommodate the ability to make a request through the posture validator to the corresponding posture collector about the posture of the target endpoint. Standard data models and protocols also enable the security of posture assessment results. By storing these results indexed under the endpoint's unique identification, secure storage itself enables endpoint posture information correlation, and ensures that the enterprise's repositories always offer the freshest, most up-to-date view of the enterprise's endpoint posture information possible.

1.7. Posture Information Can Be Shared

By exposing posture information using a standard interface and API, other security and operational components have a high level of insight into the enterprise's endpoints and the software installed on them. This will support innovation in the areas of asset management, vulnerability scanning, and administrative interfaces, as any authorized infrastructure endpoint can interact with the posture information.

1.8. Enterprise Asset Posture Information Belongs to the Enterprise

Owners and administrators must have complete control of posture information, policy, and endpoint mitigation. Standardized data models, protocols and interfaces help to ensure that this posture information is not locked in proprietary databases, but is made available to its owners. This enables administrators to develop as nuanced a policy as necessary to keep their networks secure.

1.9. Keywords

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]. This specification does not distinguish blocks of informative comments and normative requirements. Therefore, for the sake of clarity, note that lower case instances of must, should, etc. do not indicate normative requirements.

2. Terminology

This document uses terms as defined in [I-D.ietf-sacm-terminology] unless otherwise specified.

3. Assumptions

Here are the assumptions that the Endpoint Compliance Profile makes about other components in the SACM architecture.

- Existence of a posture manager and repository: The Endpoint Compliance Profile assumes that a posture manager and repository exist.

- Endpoint posture information availability: The Endpoint Compliance Profile assumes that an endpoint has posture information in standardized data model that can be communicated to the posture manager.

- Certificate provisioning: In order to implement the most secure endpoint identification option, the Endpoint Compliance Profile assumes that the enterprise has set up a certificate root authority, and has provisioned each endpoint with an endpoint identification certificate. This is not required if an enterprise chooses to use other endpoint authentication methods.

In addition, the Endpoint Compliance Profile makes the following assumptions about the SACM ecosystem:

- All network-connected endpoints are endpoints: As defined by [I-D.ietf-sacm-terminology], an endpoint is any physical or virtual computing endpoint that can be connected to a network. Posture assessment against policy is equally, if not more, important for continuously connected endpoints, such as enterprise workstations and infrastructure endpoints, as it is for sporadically connected endpoints. Continuously connected endpoints are just as likely to fall out of compliance with policy, and a standardized posture assessment method is necessary to ensure they can be properly handled.

- All endpoints on the network must be uniquely identified: Many administrators struggle to identify what endpoints are connected at any given time. By requiring a standardized method of endpoint identity, the Endpoint Compliance Profile will enable administrators to answer the basic question, "What is on my network?" Unique endpoint identification also enables the comparison of current and past endpoint posture assessments, by allowing administrators to correlate assessments from the same endpoint. This makes it easier to flag suspicious changes in endpoint posture for manual or automatic review, and helps to swiftly identify malicious changes to endpoint applications.

- Posture assessments must occur over secure, standardized protocols: Endpoint identity and application information is very valuable, both to administrators and to attackers. Therefore, it must be kept confidential, using secure protocols to transport it from the endpoint to the posture manager. Additionally, it is critical that only authorized parties be capable of requesting information, receiving information, or taking action to change an endpoint's connectivity status. Relying on standardized protocols to provide this security enables greater interoperability and compatibility between endpoints, and allows for the development of compliance testing to ensure that each endpoint operates securely and in conformance with appropriate specifications. A standards body provides a process for experts in protocols and cryptography to evaluate the soundness of protocols and security management procedures; a set of security standards allows an enterprise to make the most effective use of their investment in a security management infrastructure.

- Posture assessment results must be formatted using standardized data models: Well-known, standard data models allow for a universal language for generating compliance reports. With each endpoint speaking the same language, the Endpoint Compliance Profile enables information sharing between user endpoints and infrastructure endpoints, and between infrastructure endpoints that perform different security tasks.

- Posture information must be stored by the repository and must be exposed to an interface at the posture manager: Standard data models enable standard queries from an interface exposed to an administrator at the posture manager console. A repository must retain any current posture information retrieved from the endpoint and store it indexed by the unique identifier for the endpoint. Any posture validator specified by this profile must be able to ascertain from its corresponding posture collector whether the posture information is up to date. An interface on the posture manager must support a request to the posture validator to obtain up-to-date information when an endpoint is connected. This interface must also support the ability to make a standard set of queries about the posture information stored by the repository. In the future, some forms of posture information might be retained at the endpoint. The interface on the posture manager must accommodate the ability to make a request through the posture validator to the corresponding posture collector about the posture of the endpoint. Standard data models and protocols also enable the security of posture assessment results. By storing these results indexed under the endpoint's unique identifier, secure storage itself enables endpoint posture information correlation, and ensures that the enterprise's repositories always offer the

freshest, most up-to-date view of the enterprise's endpoint posture information possible.

- Posture information can be shared: By exposing posture information using a standard interface and API, other security and operational components have a high level of insight into the enterprise's endpoints and the software installed on them. This will support innovation in the areas of asset management, vulnerability scanning, and administrative interfaces, as any authorized infrastructure endpoint can interact with the posture information.

- Owners and administrators must have complete control of posture information, policy, and endpoint mitigation: Enterprise asset posture information belongs to the enterprise. Standardized data models, protocols and interfaces help to ensure that this posture information is not locked in proprietary databases, but is made available to its owners. This enables administrators to develop as nuanced a policy as necessary to keep their networks secure.

4. Endpoint Compliance Profile

The Endpoint Compliance Profile describes how IETF data models and protocols can be used to support the posture assessment of endpoints on a network. This profile does not generate new data models or protocols; rather, it offers a full end-to-end solution for posture assessment, as well as a fresh perspective on how existing standards can be leveraged against vulnerabilities.

4.1. Posture Assessments

The Endpoint Compliance Profile 1.0 describes how IETF and TNC data models and protocols make it possible to perform posture assessments against all network-connected endpoints by:

1. uniquely identifying the endpoint;

2. collecting and assessing posture based on data from the endpoint;

3. creating a secure, authenticated, confidential channel between the endpoint and the posture manager;

4. enabling the endpoint to notify the posture manager about changes to its configuration;

5. enabling the posture manager to request information about the configuration of the endpoint; and

6. storing the posture information in a repository linked to the identifier for the endpoint.

4.2. Data Storage

The Endpoint Compliance Profile 1.0 focuses on being able to collect posture information from an endpoint and store it in a repository. This makes posture information from a network's endpoints available to authorized parties. Uses of this data are innumerable - vulnerability management, asset management, software asset management, and configuration management solutions, analytics tools, endpoints that need to make connectivity decisions, and metrics reporting scripts, among others, are all able to reference the data stored in the repository to achieve their purposes. Currently, the Endpoint Compliance Profile 1.0 does not specify a protocol or interfaces to access stored posture information. This needs to be addressed in a future revision to make collected posture information accessible to components in a standardized manner. Until then, vendors are free to implement a repository and the protocols and interfaces used to interact with it in a way that makes the most sense for them.

4.3. Data Sharing

The Endpoint Compliance Profile 1.0 aims to facilitate the sharing of posture information between components to enable asset management, software asset management, and configuration management use cases as well as support analytic, access control, remediation, and reporting processes. However, the Endpoint Compliance Profile 1.0 does not currently specify a protocol for communicating this information between components to support these use cases and processes. This needs to be addressed in a future revision. [I-D.ietf-mile-xmpp-grid] which is publish/subscribe protocol being developed in the IETF MILE WG may be a potential candidate for sharing information between components.

5. ECP Components

To perform posture assessment, data storage, and data sharing, ECP defines a number of components. Some of these components reside on the target endpoint. Others reside on a posture manager that manages communications with the target endpoint and stores the target endpoint's posture information in a repository.

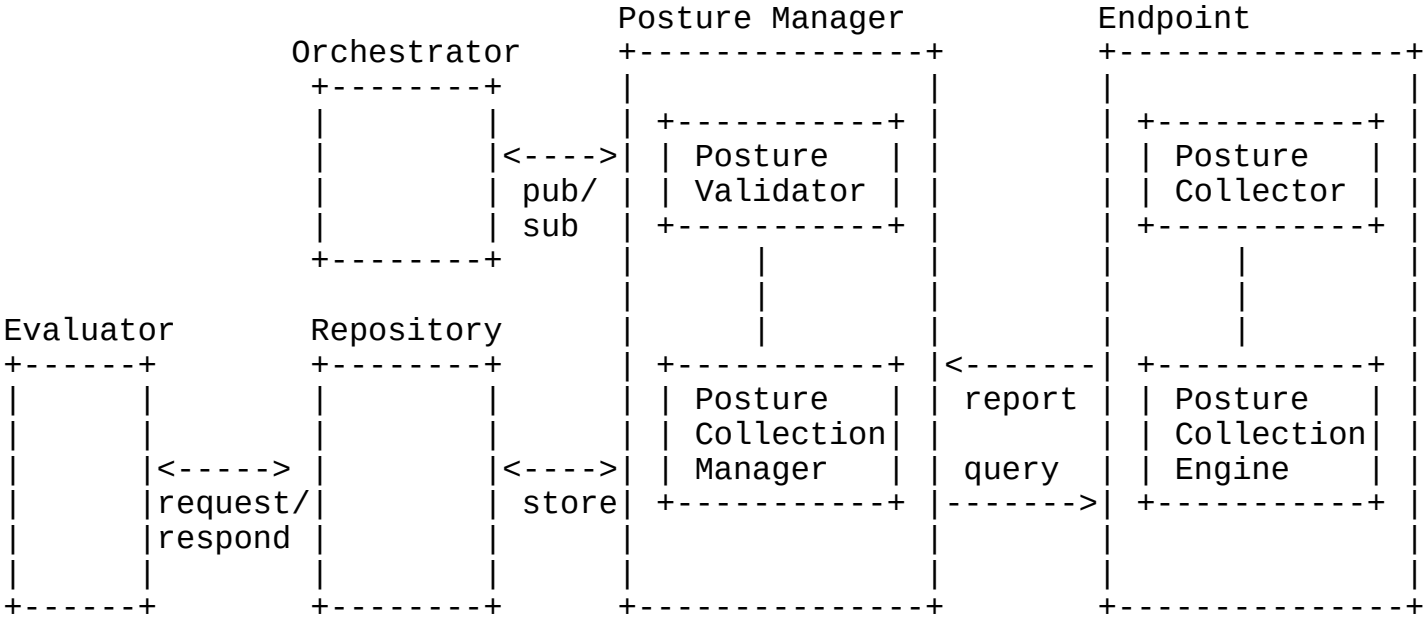

Figure 1: ECP Components

5.1. Endpoint

An endpoint is defined in [RFC6876]. In the Endpoint Compliance Profile, the endpoint is monitored by the enterprise and is the target of posture assessments. To support these posture assessments, posture information is collected via posture collectors.

5.1.1. Posture Collector

A posture collector is responsible for monitoring and gathering posture information from the target endpoint. This component reports changes to posture information as they occur. This event-driven collection provides network administrators up-to-date insight into the state of the network as the network state changes, which enables continuous monitoring of the network. Posture collectors can also be queried supporting ad-hoc collection, addressed below as "querying" which can be used to refresh information about the target endpoint, or to ask a specific question about posture information. Furthermore, a posture collector may process posture information before it is communicated to the posture manager. An endpoint may have one or more posture collectors depending on the type of endpoint and what posture information is being monitored and collected.

5.1.2. Posture Collection Engine

The posture collection engine is located on the target endpoint. It receives queries from a posture collection manager and directs them to the appropriate posture collector on the target endpoint. It also sends collected posture information to the posture manager where it can be received by the posture collection manager and distributed to the appropriate posture validator where it can be sanity checked and stored in the repository. The posture collection engine also contains a capability that sets up exchanges between the target endpoint and posture manager. This capability makes the posture collection engine responsible for performing the client-side portion of encryption handshakes, and for locating authorized posture managers with which to communicate.

5.2. Posture Manager

The posture manager is an endpoint that collects, validates, and enriches posture information received about a target endpoint. It also stores the posture information it receives in the repository. The posture manager does not evaluate the posture information.

5.2.1. Posture Validator

A posture validator receives data from a posture collector, performs basic sanity checking, and stores that data in the repository. It can also send queries to a posture collector. There is a posture validator for every posture collector.

5.2.2. Posture Collection Manager

A posture collection manager is a lightweight and extensible component that facilitates the coordination and execution of posture collection requests using collection mechanisms deployed across the enterprise. The posture collection manager may query and retrieve guidance from the repository to guide the collection of posture information from the target endpoint.

The posture collection manager also contains a capability that sets up exchanges between the target endpoint and the posture manager, and manages data sent to and from posture validators. It is also responsible for performing the server-side portion of encryption handshakes. It is also responsible for performing the server-side portion of encryption handshakes.

5.3. Repository

The repository hosts guidance, endpoint identification information, and posture information reported by target endpoints where it is made available to authorized components and persisted over a period of time set by the administrator. Information stored in the repository will be accessible to authorized parties via a standard administrative interface as well as through a standardized API. The repository may be a standalone component or may be located on the posture manager.

Currently, the Endpoint Compliance Profile does not provide a standardized interface or API for accessing the information contained within the repository. A future revision of the Endpoint Compliance Profile may specify a standardized interface and API for components to interact with the repository.

5.4. Evaluator

The evaluator assesses the posture status of a target endpoint by comparing collected posture information against the desired state of the target endpoint specified in guidance. The evaluator queries and retrieves the appropriate guidance from the repository as well as queries and retrieves the posture information required for the assessment from the repository. If the required posture information is not available in the repository, the evaluator may request the posture information from the posture collection engine, which will result in the collection of additional posture information from the target endpoint. This information is subsequently stored in the repository where it is made available to the evaluator and other components. The results of the assessment are stored in the repository where they are available to tools and administrators for follow-up actions, further evaluation, and historical purposes.

5.5. Orchestrator

The orchestrator provides a publish/subscribe interface for the repository so that infrastructure endpoints can subscribe to and receive published posture assessment results from the repository regarding endpoint posture changes.

The Endpoint Compliance Profile 1.0 does not currently define an orchestrator component nor does it specify a standardized publish/subscribe interface for this purpose. Future revisions of the Endpoint Compliance Profile may specify such an interface.

6. ECP Transactions

6.1. Provisioning

An endpoint is provisioned with one or more attributes that will serve as its unique identifier on the network as well as the components necessary to interact with the posture manager. The endpoint is deployed on the network.

NOTE: TO BE EXPANDED

6.2. Discovery and Validation

If necessary, the target endpoint finds and validates the posture manager. The posture collection engine on the target endpoint and posture collection manager on the posture manager complete a TLS handshake, during which endpoint identity information is exchanged.

6.3. Event Driven Collection

The posture assessment is initiated when a posture collector on the target endpoint notices that relevant posture information on the endpoint has changed. The posture collector notified the posture collection engine, which initiates a posture assessment information exchange with the posture collection manager.

6.4. Querying

The posture assessment is initiated by the posture validator. This can occur because:

1. policy states that a previous assessment has aged out or become invalid, or

2. the posture validator is alerted by a sensor or an administrator (via the posture manager’s user interface) that an assessment must be completed

6.5. Data Storage

Once posture information is received by the posture manager, it is forwarded to the repository. The repository could be co-located with the posture manager, or there could be direct or brokered communication between the posture manager and the repository. The posture information is stored in the repository along with past posture information collected about the target endpoint.

6.6. Data Sharing

Because the target endpoint posture information was sent in standards-based data models over secure, standardized protocols, and then stored in a centralized repository linked to unique endpoint identifiers, authorized parties are able to access the posture information. Such authorized parties may include, but are not limited to, administrators or endpoint owners (via the server's administrative interface), evaluators that access the repository directly, and orchestrators that rely on publish/subscribe communications with the repository.

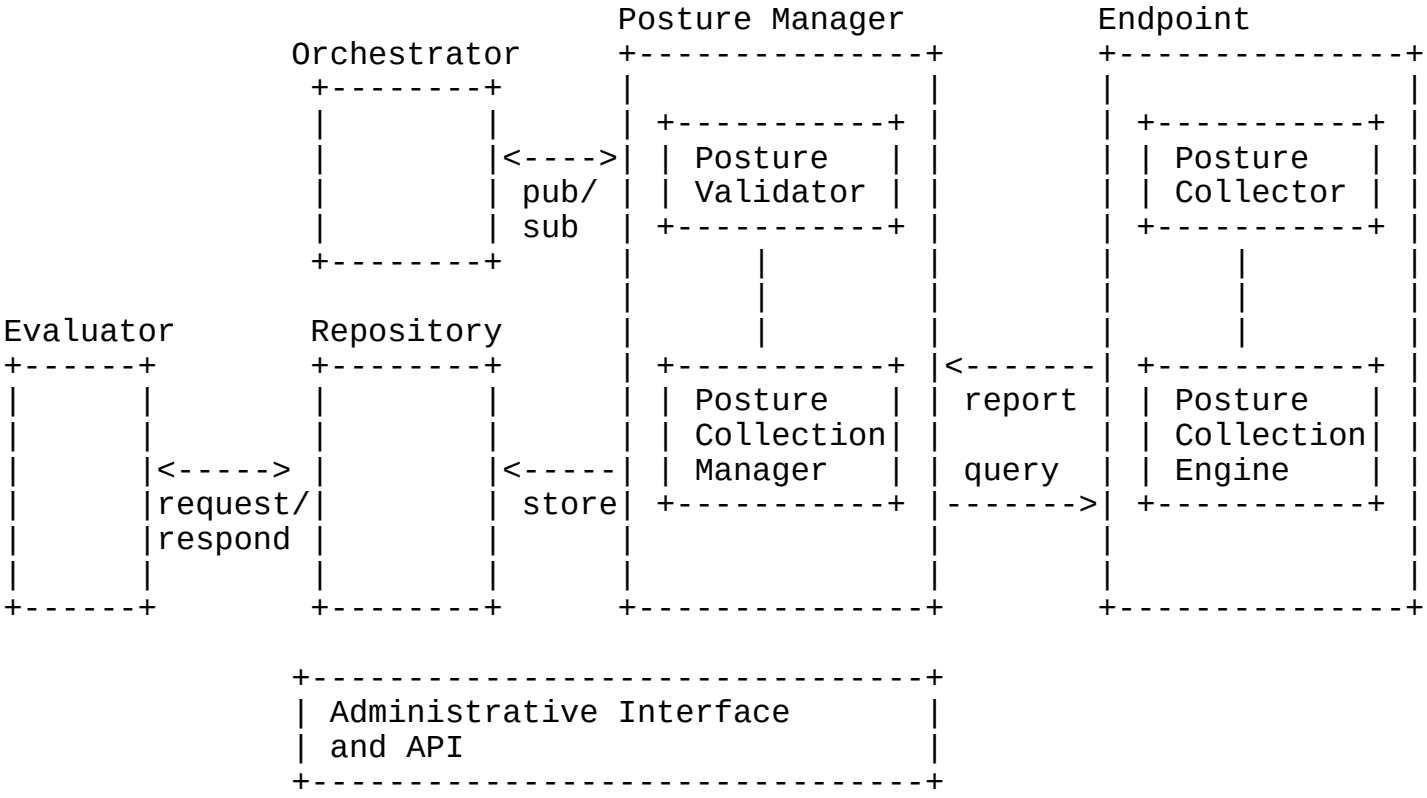

Figure 2: Exposing Data to the Network

It should be noted that the neither the Endpoint Compliance Profile nor the protocols, interfaces, and data models that it references provide solutions to the repository, evaluator, and orchestrator components and capabilities listed above. However, these capabilities are useful and solutions for them should be pursued in the future.

7. ECP Implementations

The following sections describe implementations of the Endpoint Compliance Profile leveraging the IETF NEA and IETF NETMOD architectures.

7.1. IETF NEA ECP Implementation

These requirements are written with a view to performing a posture assessment on an endpoint; as the Endpoint Compliance Profile grows and evolves, these requirements will be expanded to address issues that arise. Note that these requirements refer to defined components of the NEA architecture. As with the NEA architecture, vendors have discretion as to how these NEA components map to separate pieces of software or endpoints.

7.1.1. Endpoint Pre-Provisioning

An endpoint is provisioned with a machine certificate that will serve as its unique identifier on the network as well as the components necessary to interact with the posture manager. This includes a posture collection engine to manage requests from the posture manager and the posture collectors necessary to collect the posture information of importance to the enterprise. The endpoint is deployed on the network.

The target endpoint SHOULD authenticate to the posture manager using a machine certificate during the establishment of the outer tunnel achieved with the posture transport protocol defined in [RFC6876]. [IF-IMV] specifies how to pull an endpoint identifier out of a machine certificate. An endpoint identifier SHOULD be created in conformance with [IF-IMV] from a machine certificate sent via [RFC6876].

In the future, the identity could be a hardware certificate compliant with [IEEE-802-1ar]; ideally, this identifier SHOULD be associated with the identity of a hardware cryptographic module, in accordance with [IEEE-802-1ar], if present on the endpoint. The enterprise SHOULD stand up a certificate root authority; install its root certificate on endpoints and on the posture manager; and provision the endpoints and the posture manager with machine certificates. The target endpoint MAY authenticate to the posture manager using a combination of the machine account and password; however, this is less secure and not recommended.

7.1.2. Endpoint

The endpoint MUST conform to [RFC5793], which levies a number of requirements against the endpoint. An endpoint that complies with these requirements will be able to:

1. attempt to initiate a session with the posture manager if the posture makes a request to send an update to posture manager;

2. notify the posture collector if no PT-TLS session with the posture manager can be created;

3. notify the posture collector when a PT-TLS session is established; and

4. receive information from the posture collectors, forward this information to the server via the posture collection engine.

7.1.2.1. Posture Collector

Any posture collector used in an Endpoint Compliance Profile solution MUST be conformant with [IF-IMC]; an Internet-Draft, under development, that is a subset of the TCG TNC Integrity Measurement Collector interface [IF-IMC] and will be submitted in the near future.

7.1.2.2. Posture Collection Engine

In the original IETF NEA ECP implementation, the endpoint contained posture collector(s), a posture broker client, and posture transport client(s). However, in this draft, the functionality of the posture broker client and posture transport client(s) have been combined into what is now called the posture collection engine. This was done because there is currently no standard interface to handle the communication between the posture broker client and posture transport client(s) meaning vendors will need to define proprietary interfaces that will not be interoperable.

The endpoint MUST conform to [IF-IMC] to enable communications between the posture collection engine and the posture collectors on the endpoint.

The posture collection engine MUST implement PT-TLS.

The posture collection engine MUST support the use of machine certificates for TLS at each endpoint consistent with the requirements stipulated in [RFC6876] and [Server-Discovery].

The posture collection engine MUST be able to locate an authorized posture manager, and switch to a new posture manager when required by the network, in conformance with [Server-Discovery].

7.1.3. Posture Manager

The posture manager MUST conform to all requirements in the [RFC5793].

7.1.3.1. Posture Validator

Any posture validator used in an Endpoint Compliance Profile solution MUST be conformant with [IF-IMV]; an Internet-Draft, under development, that is a subset of the TCG TNC Integrity Measurement Verifier interface [IF-IMV] and will be submitted in the near future.

7.1.3.2. Posture Collection Manager

In the original IETF NEA ECP implementation, the posture manager contained posture validators(s), a posture broker server, and posture transport servers(s). Similar to the approach take on the endpoint, in this draft, the functionality of the posture broker server and posture transport servers(s) have been combined into what is now called the posture collection manager. This was done because there is currently no standard interface to handle the communication between the posture broker server and posture transport servers(s) meaning vendors will need to define proprietary interfaces that will not be interoperable.

The posture manager MUST conform to [IF-IMV]. Conformance to [IF-IMV] enables the posture manager to obtain endpoint identity information from the posture collection manager, and pass this information to any posture validators on the posture manager.

The posture collection manager MUST implement PT-TLS.

The posture collection manager MUST support the use of machine certificates for TLS at each endpoint consistent with the requirements stipulated in [RFC6876] and [Server-Discovery].

7.1.4. Repository

ECP 1.0 requires a simple administrative interface for the repository. Posture validators on the posture manager receive the target endpoint posture information via PA-TNC [RFC5792] messages sent from corresponding posture collectors on the target endpoint and store this information in the repository linked to the identity of the target endpoint where the posture collectors are located.

7.1.5. Administrative Interface and API

An interface is necessary to allow administrators to manage the endpoints and software used in the Endpoint Compliance Profile. This interface SHOULD be accessible either on or through (as in the case of a remotely hosted interface) the posture manager. Using this interface, an authorized user or administrator SHOULD be able to:

- Query the repository
- Send commands to the posture validators, requesting information from the associated posture collectors residing on network endpoints
- Update the policy that resides on the posture manager

An API is necessary to allow infrastructure endpoints and software access to the information stored in the repository. Using this API, an authorized endpoint SHOULD be able to:

- Query the repository

7.1.6. IETF SACM SWAM Extension to the IETF NEA ECP Implementation

This section defines the requirements associated with the software asset management extension [I-D.ietf-sacm-nea-swima-patnc] to the IETF NEA ECP implementation.

7.1.6.1. Endpoint Pre-Provisioning

This section defines the requirements associated with implementing SWIMA.

The following requirements assume that the platform or OS vendor supports the use of SWID tags and has identified a standard directory location for the SWID tags to be located as specified by [SWID].

7.1.6.2. SWID Tags

The primary content for the Endpoint Compliance Profile 1.0 is the information conveyed in the elements of a SWID tag.

The endpoint MUST have SWID tags stored in a directory specified in [SWID]. The tags SHOULD be provided by the software vendor; they MAY also be generated by:

- the software installer; or

- o third-party software that creates tags based on the applications it sees installed on the endpoint.

The elements in the SWID tag MUST be populated as specified in [SWID]. These tags, and the directory in which they are stored, MUST be updated as software is added, removed, or updated.

7.1.6.3. SWID Posture Collectors and Posture Validators

7.1.6.3.1. The SWID Posture Collector

For the Endpoint Compliance Profile, the SWID posture collector MUST be conformant with [I-D.ietf-sacm-nea-swima-patnc], which includes requirements for:

1. Collecting SWID tags from the SWID directory
2. Monitoring the SWID directory for changes
3. Initiating a session with the posture manager to report changes to the directory
4. Maintaining a list of changes to the SWID directory when updates take place and no PT-TLS connection can be created with the posture manager
5. Responding to a request for SWID tags from the SWID Posture Validator on the posture manager
6. Responding to a query from the SWID posture validator as to whether all updates have been sent

The SWID posture collector is not responsible for detecting that the SWID directory was not updated when an application was either installed or uninstalled.

7.1.6.3.2. The SWID Posture Validator

Conformance to [I-D.ietf-sacm-nea-swima-patnc] enables the SWID posture validator to:

1. Send messages to the SWID posture collector (at the behest of the administrator at the posture manager console) requesting updates for SWID tags located on endpoint
2. Ask the SWID posture collector whether all updates to the SWID directory located at the posture manager have been sent

3. Compare an endpoint’s SWID posture information to policy, and make a recommendation to the NEA server about the endpoint

In addition to these requirements, a SWID posture validator used in conformance with this profile MUST be capable of passing information from the posture assessment results and the endpoint identity associated with those results to the repository for storage.

7.1.6.4. Repository

The administrative interface SHOULD enable an administrator to:

1. Query which endpoints have reported SWID tags for a particular application

2. Query which SWID tags are installed on an endpoint

3. Query tags based on characteristics, such as vendor, publisher, etc.

7.2. IETF NETMOD ECP Implementation

NOTE: TO BE WRITTEN

8. ECP Use Cases

The following sections describe the different use cases supported by the Endpoint Compliance Profile.

8.1. Hardware Asset Management

Using the administrative interface on the posture manager, an authorized user can learn:

- what endpoints are connected to the network at any given time; and

- what SWID tags were reported for the endpoints.

The ability to answer these questions offers a standards-based approach to asset management, which is a vital part of enterprise processes such as compliance report generation for the Federal Information Security Modernization Act (FISMA), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), etc.

8.2. Software Asset Management

The administrative interface on the posture manager provides the ability for authorized users and infrastructure to know which software is installed on which endpoints on the enterprise's network. This allows the enterprise to answer questions about what software is installed to determine if it is licensed or prohibited. This information can also drive other use cases such as:

- vulnerability management: knowing what software is installed supports the ability to determine which endpoints contain vulnerable software and need to be patched.

- configuration management: knowing which security controls need to be applied to harden installed software and better protect endpoints.

8.3. Vulnerability Searches

The administrative interface also provides the ability for authorized users or infrastructure to locate endpoints running software for which vulnerabilities have been announced. Because of

1. the unique IDs assigned to each endpoint; and

2. the rich application data provided in the endpoints' posture information,

the repository can be queried to find all endpoints running a vulnerable application. Endpoints suspected of being vulnerable can be addressed by the administrator or flagged for further scrutiny.

8.4. Threat Detection and Analysis

The repository's standardized API allows authorized infrastructure endpoints and software to search endpoint posture assessment information for evidence that an endpoint's software inventory has changed, and can make endpoint software inventory data available to other endpoints. This automates security data sharing in a way that expedites the correlation of relevant network data, allowing administrators and infrastructure endpoints to identify odd endpoint behavior and configuration using secure, standards-based data models and protocols.

9. Non-supported Use Cases

Several use cases, including but not limited to these, are not covered by the Endpoint Compliance Profile 1.0:

- Gathering non-standardized types of posture information: The Endpoint Compliance Profile does not prevent administrators from collecting posture information in proprietary formats from the endpoint; however it does not set requirements for doing so.

- Solving the lying endpoint problem: The Endpoint Compliance Profile does not address the lying endpoint problem; the Profile makes no assertions that it can catch an endpoint that is, either maliciously or accidentally, reporting false posture information to the posture manager. However, other solutions may be able to use the posture information collected using the capabilities described in this profile to catch an endpoint in a lie. For example, a sensor may be able to compare the posture information it has collected on an endpoint's activity on the network to what the endpoint reported to the server and flag discrepancies. However, these capabilities are not described in this profile.

10. Endpoint Compliance Profile Examples

10.1. Continuous Posture Assessment of an Endpoint

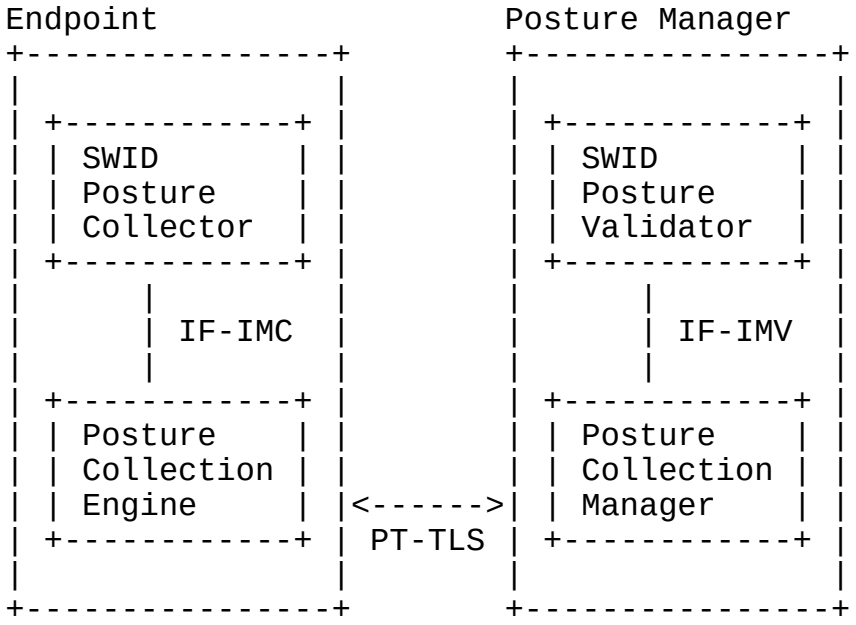

Figure 3: Continuous Posture Assessment of an Endpoint

10.1.1. Change on Endpoint Triggers Posture Assessment

A new application is installed on the endpoint, and the SWID directory is updated. This triggers an update from the SWID posture collector to the SWID posture validator. The message is sent down the NEA stack, encapsulated by NEA protocols until it is sent by the posture transport client to the posture transport server. The posture transport server then forwards it up through the stack, where the layers of encapsulation are removed until the SWID Message arrives at the SWID posture validator.

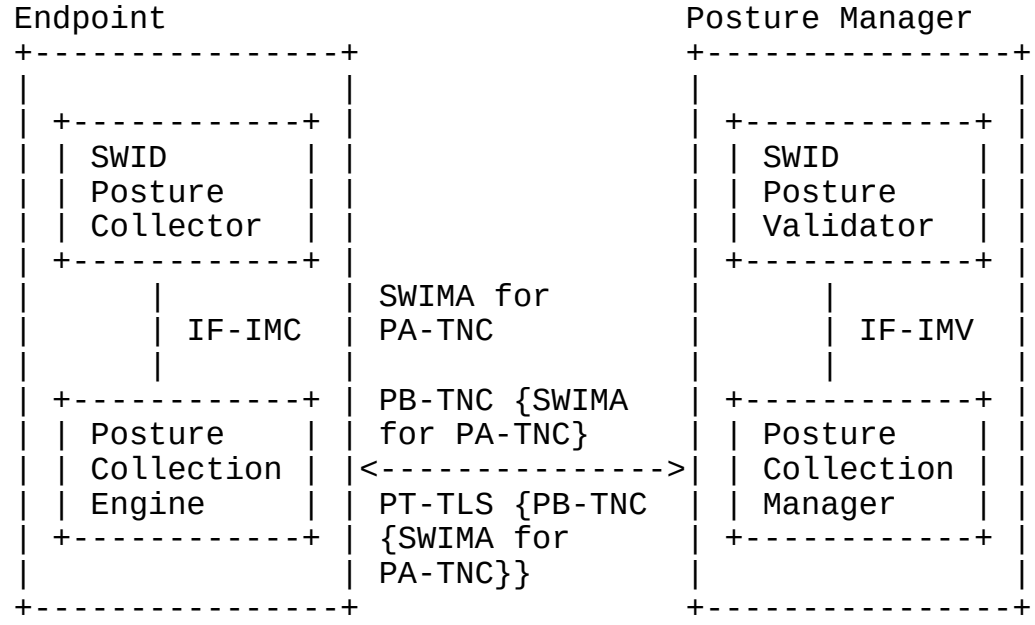

Figure 4: Compliance Protocol Encapsulation

The SWID posture validator stores the new tag information in the repository. If the tag indicates that the endpoint is compliant to the policy, then the process is complete until the next time an update is needed (either because policy states that the endpoint must submit posture assessment results periodically or because an install/uninstall/update on the endpoint triggers a posture assessment).

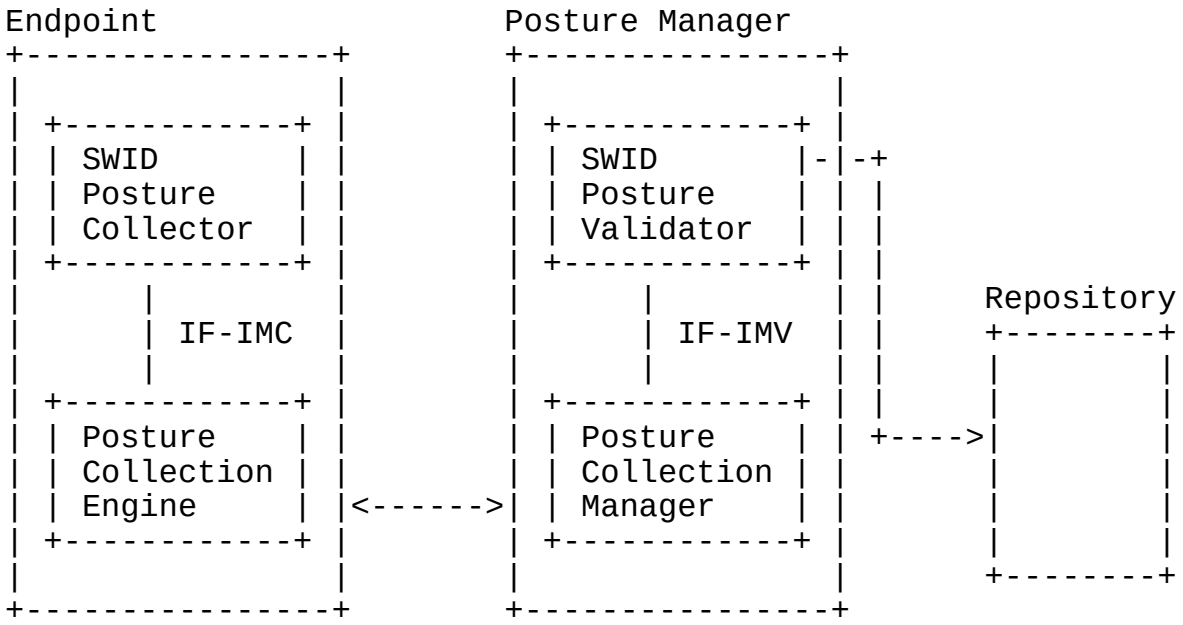

Figure 5: Storing SWIDs in the Repository

If the endpoint has fallen out of compliance with a policy, the server can alert the administrator via the posture manager's administrative interface. The administrator can then take steps to address the problem. If the administrator has already established a policy for automatically addressing this problem, that policy will be followed.

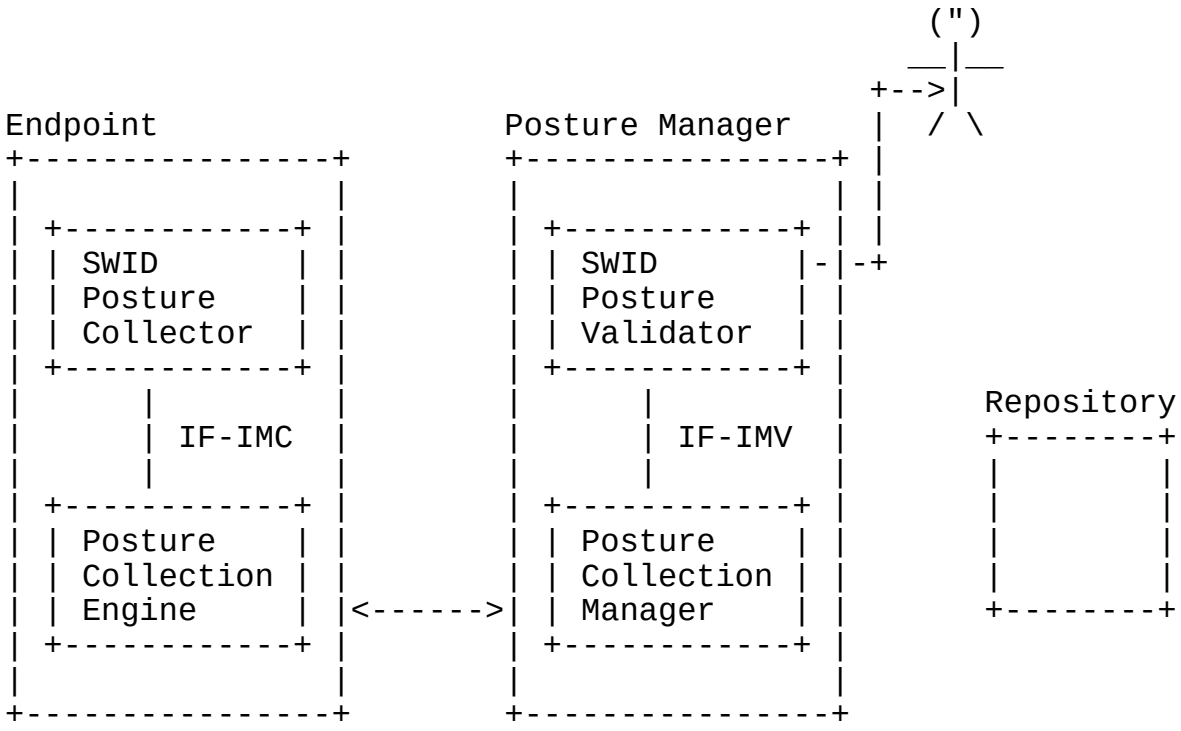

Figure 6: Server Alerts Network Admin

10.2. Administrator Searches for Vulnerable Endpoints

An announcement is made that a particular version of a piece of software has a vulnerability. The administrator uses the Administrative Interface on the server to search the repository for endpoints that reported the SWID tag for the vulnerable software.

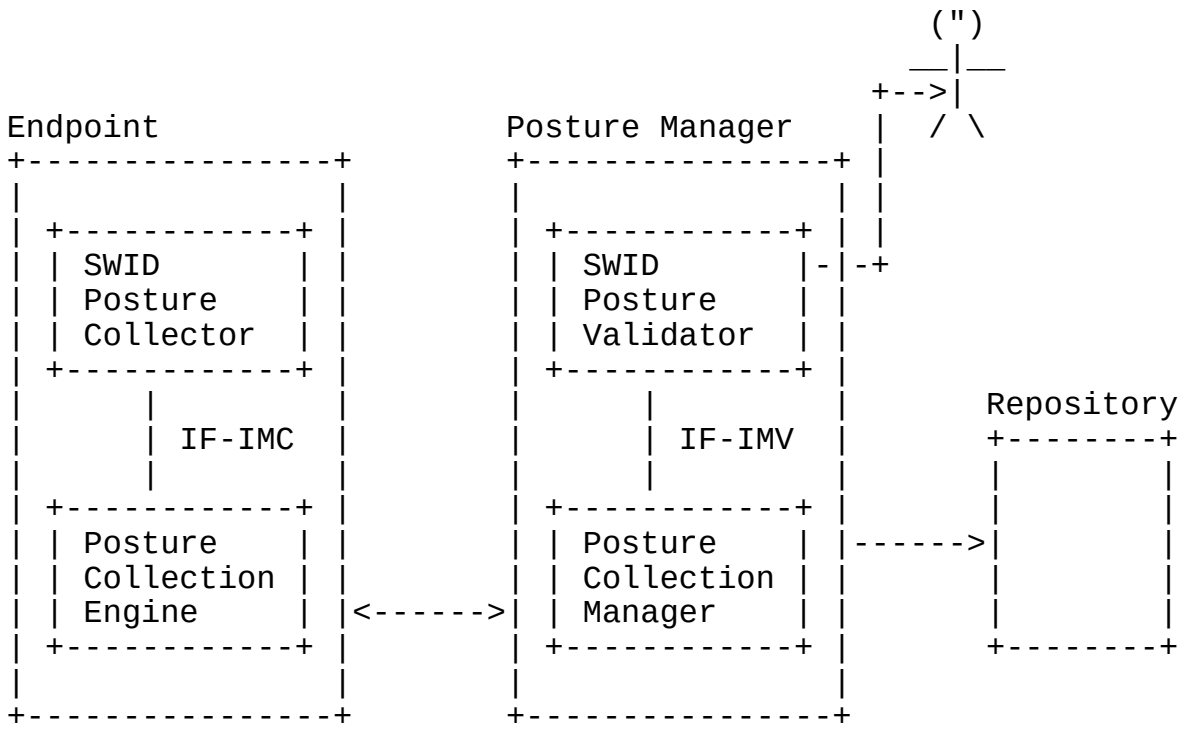

Figure 7: Admin Searches for Vulnerable Endpoints

The repository returns a list of entries in the matching the administrator's search. The administrator can then address the vulnerable endpoints by taking some follow-up action such as removing it from the network, quarantining it, or updating the vulnerable software.

11. Profile Requirements

Here are the requirements that the Endpoint Compliance Profile protocol must meet in order to successfully fit in the SACM architecture.

- Meets the needs of SACM use cases: The Endpoint Compliance Profile must support the use cases described in [RFC7632] as they apply to endpoint self-reporting and endpoint posture assessment.

- Efficient: To minimize user frustration, it is essential to minimize delays by making endpoint posture information collection, transmission, and assessment as brief and efficient as possible.

- Extensible: The Endpoint Compliance Profile needs to expand over time as new features are added to the SACM architecture. The solution must allow new features to be added easily, providing for a smooth transition and allowing newer and older architectural

components to continue to work together. Further, the Endpoint Compliance Profile and the specifications referenced here must define safe extensibility mechanisms that enable innovation without breaking interoperability.

- Easy to implement: The Endpoint Compliance Profile should be easy for vendors to implement in their products, and should result in products that are easy for administrators to implement on their networks. Products conformant to the Endpoint Compliance Profile should interoperate seamlessly, and be simple to integrate into existing network infrastructure.

- Easy to use: The Endpoint Compliance Profile should describe a simple, integrated user interface that administrators can use to perform the activities listed in the profile's use cases. The Endpoint Compliance Profile should not constrain innovation by specifying details of the user interface but rather functional requirements.

- Platform-independent: Since network environments may contain many different types of endpoints, the solution should operate independently of the endpoint platform.

- Scalable: The Endpoint Compliance Profile must be designed to scale to very large numbers of endpoints.

12. Future Work

This section captures ideas for future work related to ECP that might be of interest to the IETF SACM WG. These ideas are listed in no particular order.

- Integratate the IETF NETMOD Yang Push architecture.

- Add support endpoint types beyond workstations, servers, and network infrastructure devices.

- Examine the integration of [I-D.ietf-mile-xmpp-grid].

- Define a standard interface and API for interacting with the repository. Requirements to consider include: creating a secure channel between a publisher and the repository, creating a secure channel between a subscriber and the repository, and the types of interactions that must be supported between publishers and subscribers to a repository.

- Define a standard interface for communications between the posture broker client and posture transport client(s) as well as the posture broker server and posture transport server(s).
- Retention of posture information on the target endpoint.
- Define an orchestrator component as well as publish/subscribe interface for it.
- Define an evaluator component as well as an interface for it.

13. Acknowledgements

The authors wish to thank all of those in the TCG TNC work group who contributed to development of the TNC ECP specification upon which this document is based.

Member	Organization
Padma Krishnaswamy	Battelle Memorial Institute
Eric Fleischman	Boeing
Richard Hill	Boeing
Steven Venema	Boeing
Nancy Cam-Winget	Cisco Systems
Scott Pope	Cisco Systems
Max Pritikin	Cisco Systems
Allan Thompson	Cisco Systems
Nicolai Kuntze	Fraunhofer Institute for Secure Information Technology (SIT)
Ira McDonald	High North
Dr. Andreas Steffen	HSR University of Applied Sciences Rapperswil
Josef von Helden	Hochschule Hannover
James Tan	Infoblox

Steve Hanna (TNC-WG Co-Chair)	Juniper Networks
Cliff Kahn	Juniper Networks
Lisa Lorenzin	Juniper Networks
Atul Shah (TNC-WG Co-Chair)	Microsoft
Jon Baker	MITRE
Charles Schmidt	MITRE
Rainer Enders	NCP Engineering
Dick Wilkins	Phoenix Technologies
David Waltermire	NIST
Mike Boyle	U.S. Government
Emily Doll	U.S. Government
Jessica Fitzgerald-McKay	U.S. Government
Mary Lessels	U.S. Government
Chris Salter	U.S. Government

Table 1: Members of the TNC Work Group that Contributed to the Document

14. IANA Considerations

This document does not define any new IANA registries. However, this document does reference other documents that do define IANA registries. As a result, the IANA Considerations section of the referenced documents should be consulted.

15. Security Considerations

The Endpoint Compliance Profile offers substantial improvements in endpoint security, as evidenced by the Australian Defense Signals Directorate’s analysis that 85% of targeted cyber intrusions can be prevented through application whitelisting, patching applications and

operating systems, and using the latest versions of applications. [DSD] Despite these gains, some security risks continue to exist and must be considered.

To ensure that these benefits and risks are properly understood, this Security Considerations section includes an analysis of the benefits provided by the Endpoint Compliance Profile (Section 15.1), the attacks that may be mounted against systems that implement the Endpoint Compliance Profile (Section 15.2), and the countermeasures that may be used to prevent or mitigate these attacks (Section 15.3). Overall, a substantial reduction in cyber risk can be achieved.

15.1. Security Benefits of Endpoint Compliance Profile

Security weaknesses of the components for this profile should be considered in light of the practical considerations that must be addressed to have a viable solution.

Posture assessment has two parts: assessment and follow-up actions. The point of posture assessment is to ensure that authorized users are using authorized software configured to be as resilient as possible against an attack.

Posture assessment answers the question whether the endpoint is healthy. Our goal for posture assessment is to make it harder for an adversary to execute code on one of our endpoints. This profile represents an important first step in reaching that goal. If we keep our endpoints healthier, we are able to prevent more attacks on our endpoints and thus on our information systems.

The goal of ECP is to address posture assessment in stages. Stage 1 is the ability to ascertain whether all endpoints are authorized and whether all applications are authorized and up to date. Stage 2 will attempt to address the harder problem of whether all software is configured safely. Eventually, the goal is to also address remediation which is currently out-of-scope for the SACM WG; that presents a far greater security challenge than reporting, since remediation implies the ability of a remote party to modify software or its settings on endpoints.

A second security consideration is how to gain visibility over every type of endpoint and every piece of software installed on the endpoint. This is a problem of scaling and observation. A solution is needed that can report from every type of endpoint. All software on the endpoint has to be discovered. Information about the software has to be up to date and accurate. The information that is discovered has to be reported in a consistent format, so administrators do not have to squander time deciphering proprietary

systems and the information can be made readily useful for other security automation purposes.

ECP is based on a model of a standards-based schema, a standards-based set of protocols and interfaces, and the existence of an oversight group, the IETF, that can update the data models and protocols to meet new use cases and security issues that may be discovered.

The data elements in the schema determine what work can be done consistently for every endpoint and every piece of software. How the data gets populated is an important consideration. ECP leverages the SWID tags from ISO 19770-2 because the tag originates with a single authoritative source, the application vendor itself. Moreover, there is a natural incentive for the vendor to create this content, since it makes it easier for enterprises and vendors to track whether software is licensed. Practical considerations are security considerations. A sustainable business model for obtaining all the necessary content is a fundamental requirement.

The NEA model is based on having a NEA client run on an endpoint that publishes posture information to a server. The advantages are easy to list. A platform vendor can implement its own NEA client and have it be compatible with the NEA server from a different vendor. The interfaces are layered on top of mature protocols such as TLS. TLS is the protocol of choice for ECP, since:

- it has proven secure properties,
- it can be implemented on most types of endpoints,
- it allows the gathering of large amounts of information when a endpoint is connected, and
- it enables use of a mechanism to ensure that the client is authenticated (authorized) - a client certificate - which also provides a consistent identifier.

Mature protocols that can be implemented on most types of endpoints and a standards-based schema with a sustainable business model are both critical security considerations for compliance.

Additionally, it is important to consider the future stages for ECP such as a posture assessment being followed up by some action (e.g. remediation, alert, etc.). Ensuring that clients are taking instructions only from authorized parties will be critical. Inasmuch as it is practical, enterprises will want to use the same

infrastructure and investment in PKI to send those instructions to a client.

Likewise, as more information with more value is gathered from endpoints, we will also want to ensure that this information is only released to authorized applications and parties. For the next stage of ECP, SACM may want to define an interface on the repository that can be queried by other security automation applications to make it easier to detect attacks and for other security automation applications. This interface has to be standards-based for enterprises to reap the benefits of innovation that can be achieved by making the enterprise's data available to other tools and services.

15.2. Threat Model

This section lists the attacks that can be mounted on an Endpoint Compliance Profile environment. The following section (Section 15.3) describes countermeasures.

Because the Endpoint Compliance Profile describes a specific use case for NEA components, many security considerations for these components are addressed in more detail in the technical specifications: [I-D.ietf-sacm-nea-swima-patnc], [IF-IMC], [RFC5793], [Server-Discovery], [RFC6876], [IF-IMV].

15.2.1. Endpoint Attacks

While the Endpoint Compliance Profile provides substantial improvements in endpoint security as described in Section 15.1, a certain percentage of endpoints will always get compromised. For this reason, all parties must regard data coming from endpoints as potentially unreliable or even malicious. An analogy can be drawn with human testimony in an investigation or trial. Human testimony is essential but must be regarded with suspicion.

- Compromise of endpoint: A compromised endpoint may report false information to confuse or even provide maliciously crafted information with a goal of infecting others.

- Putting bad information in SWID directory: Even if an endpoint is not completely compromised, some of the software running on it may be unreliable or even malicious. This software, potentially including the SWID generation or discovery tool, or malicious software pretending to be a SWID generation or discovery tool, can place incorrect or maliciously crafted information into the SWID directory. Endpoint users may even place such information in the

directory, whether motivated by curiosity or confusion or a desire to bypass restrictions on their use of the endpoint.

- Identity spoofing (impersonation): A compromised endpoint may attempt to impersonate another endpoint to gain its privileges or to besmirch the reputation of that other endpoint.

15.2.2. Network Attacks

A variety of attacks can be mounted using the network. Generally, the network cannot be trusted.

- Eavesdropping, modification, injection, replay, deletion
- Traffic analysis
- Denial of service and blocking traffic

15.2.3. Posture Manager Attacks

The posture manager is a critical security element and therefore merits considerable scrutiny.

- Compromised trusted manager: A compromised posture manager or a malicious party that is able to impersonate a posture manager can incorrectly grant or deny access to endpoints, place incorrect information into the repository, or send malicious messages to endpoints.
- Misconfiguration of posture manager: Accidental or purposeful misconfiguration of a trusted posture manager can cause effects that are similar to those listed for compromised trusted posture manager.
- Malicious untrusted posture manager: An untrusted posture manager cannot mount any significant attacks because all properly implemented endpoints will refuse to engage in any meaningful dialog with such a posture manager.

15.2.4. Repository Attacks

The repository is also an important security element and therefore merits careful scrutiny.

- Putting bad information into trusted repository: An authorized repository client such as a server may be able to put incorrect information into a trusted repository or delete or modify historical information, causing incorrect decisions about endpoint

security. Placing maliciously crafted data in the repository could even lead to compromise of repository clients, if they fail to carefully check such data.

- Compromised trusted repository: A compromised trusted repository or a malicious untrusted repository that is able to impersonate a trusted repository can lead to effects similar to those listed for "Putting bad information into trusted repository". Further, a compromised trusted repository can report different results to different repository clients or deny access to the repository for selected repository clients.

- Misconfiguration of trusted repository: Accidental or purposeful misconfiguration of a trusted repository can deny access to the repository or result in loss of historical data.

- Malicious untrusted repository: An untrusted repository cannot mount any significant attacks because all properly implemented repository clients will refuse to engage in any meaningful dialog with such a repository.

15.3. Countermeasures

This section lists the countermeasures that can be used in an Endpoint Compliance Profile environment.

15.3.1. Countermeasures for Endpoint Attacks

This profile is in and of itself a countermeasure for a compromised endpoint. A primary defense for an endpoint is to run up to date software configured to be run as safely as possible.

Ensuring that anti-virus signatures are up to date and that a firewall is configured are also protections for an endpoint that are supported by the current NEA specifications.

Endpoints that have hardware cryptographic modules that are provisioned by the enterprise, in accordance with [IEEE-802-1ar], can protect the private keys used for authentication and help prevent adversaries from stealing credentials that can be used for impersonation. Future versions of the Endpoint Compliance Profile may want to discuss in greater detail how to use a hardware cryptographic module, in accordance with [IEEE-802-1ar], to protect credentials and to protect the integrity of the code that executes during the bootstrap process.

15.3.2. Countermeasures for Network Attacks

To address network attacks, [RFC6876] includes required encryption, authentication, integrity protection, and replay protection. [Server-Discovery] also includes authorization checks to ensure that only authorized servers are trusted by endpoints. Any unspecified or not yet specified network protocols employed in the Endpoint Compliance Profile (e.g. the protocol used to interface with the repository) should include similar protections.

These protections reduce the scope of the network threat to traffic analysis and denial of service. Countermeasures for traffic analysis (e.g. masking) are usually impractical but may be employed. Countermeasures for denial of service (e.g. detecting and blocking particular sources) SHOULD be used when appropriate to detect and block denial of service attacks. These are routine practices in network security.

15.3.3. Countermeasures for Posture Manager Attacks

Because of the serious consequences of posture manager compromise, posture managers SHOULD be especially well hardened against attack and minimized to reduce their attack surface. They SHOULD be monitored using the NEA protocols to ensure the integrity of the behavior and analysis data stored on the posture manager and SHOULD utilize a [IEEE-802-1ar]compliant hardware cryptographic module for identity and/or integrity measurements of the posture manager. They should be well managed to minimize vulnerabilities in the underlying platform and in systems upon which the posture manager depends. Network security measures such as firewalls or intrusion detection systems may be used to monitor and limit traffic to and from the posture manager. Personnel with administrative access to the posture manager should be carefully screened and monitored to detect problems as soon as possible. Posture manager administrators should not use password-based authentication but should instead use non-reusable credentials and multi-factor authentication (where available). Physical security measures should be employed to prevent physical attacks on posture managers.

To ease detection of posture manager compromise should it occur, posture manager behavior should be monitored to detect unusual behavior (such as a server reboot, unusual traffic patterns, or other odd behavior). Endpoints should log and/or notify users and/or administrators when peculiar posture manager behavior is detected. To aid forensic investigation, permanent read-only audit logs of security-relevant information pertaining to posture manager (especially administrative actions) should be maintained. If posture manager compromise is detected, the posture manager’s certificate

should be revoked and careful analysis should be performed of the source and impact of this compromise. Any reusable credentials that may have been compromised should be reissued.

Endpoints can reduce the threat of server compromise by minimizing the number of trusted posture managers, using the mechanisms described in [Server-Discovery].

15.3.4. Countermeasures for Repository Attacks

If the host for the repository is located on its own endpoint, it should be protected with the same measures taken to protect the posture manager. In this circumstance, all messages between the posture manager and repository should be protected with a mature security protocol such as TLS or IPsec.

The repository can aid in the detection of compromised endpoints if an adversary cannot tamper with its contents. For instance, if an endpoint reports that it does not have an application with a known vulnerability installed, an administrator can check whether the endpoint might be lying by querying the repository for the history of what applications were installed on the endpoint.

To help prevent tampering with the information in the repository:

1. Only authorized parties should have privilege to run code on the endpoint and to change the repository.

2. If a separate endpoint hosts the repository, then the functionality of that endpoint should be limited to hosting the repository. The firewall on the repository should only allow access to the posture manager and to any endpoint authorized for administration.

3. The repository should ideally use "write once" media to archive the history of what was placed in the repository, to include a snapshot of the current status of applications on endpoints.

16. Privacy-Considerations

The Endpoint Compliance Profile specifically addresses the collection of posture data from enterprise endpoints by an enterprise network. As such, privacy is not going to often arise as a concern for those deploying this solution.

A possible exception may be the concerns a user may have when attempting to connect a personal endpoint (such as a phone or mobile endpoint) to an enterprise network. The user may not want to share

certain details, such as an endpoint identifier or SWID tags, with the enterprise. The user can configure their NEA client to reject requests for this information; however, it is possible that the enterprise policy will not allow the user's endpoint to connect to the network without providing the requested data.

17. Change Log

17.1. -00 to -01

There are no textual changes associated with this revision. This revision simply reflects a resubmission of the document so that it remains in active status.

17.2. -01 to -02

Added references to the Software Inventory Message and Attributes (SWIMA) for PA-TNC I-D.

Replaced references to PC-TNC with IF-IMC.

Removed erroneous hyphens from a couple of section titles.

Made a few minor editorial changes.

17.3. -02 to -00

Draft adopted by IETF SACM WG.

17.4. -00 to -01

Significant edits to up-level the draft to describe SACM collection over multiple different protocols.

Replaced references to SANS with CIS.

Made other minor editorial changes.

18. References

18.1. Informative References

[CIS] http://www.cisecurity.org/controls/, "CIS Critical Security Controls".

[DSD] http://www.dsd.gov.au/publications/csocprotect/top_4_mitigations.htm, "Top 4 Mitigation Strategies to Protect Your ICT System", November 2012.

[IEEE-802-1ar]
Institute of Electrical and Electronics Engineers, "IEEE 802.1ar", December 2009.

[RFC5209] Sangster, P., Khosravi, H., Mani, M., Narayan, K., and J. Tardo, "Network Endpoint Assessment (NEA): Overview and Requirements", RFC 5209, DOI 10.17487/RFC5209, June 2008, <https://www.rfc-editor.org/info/rfc5209>.

[TNC] Trusted Computing Group, "TCG Trusted Network Connect TNC Architecture for Interoperability, Version 1.5", February 2012.

18.2. Normative References

[I-D.ietf-mile-xmpp-grid]
Cam-Winget, N., Appala, S., Pope, S., and P. Saint-Andre, "Using XMPP for Security Information Exchange", draft-ietf-mile-xmpp-grid-04 (work in progress), October 2017.

[I-D.ietf-netconf-yang-push]
Clemm, A., Voit, E., Prieto, A., Tripathy, A., Nilsen-Nygaard, E., Bierman, A., and B. Lengyel, "YANG Datastore Subscription", draft-ietf-netconf-yang-push-12 (work in progress), December 2017.

[I-D.ietf-sacm-nea-swima-patnc]
Schmidt, C., Haynes, D., Coffin, C., Waltermire, D., and J. Fitzgerald-McKay, "Software Inventory Message and Attributes (SWIMA) for PA-TNC", draft-ietf-sacm-nea-swima-patnc-01 (work in progress), September 2017.

[I-D.ietf-sacm-terminology]
Waltermire, D., Montville, A., Harrington, D., and N. Cam-Winget, "Terminology for Security Assessment", draft-ietf-sacm-terminology-05 (work in progress), August 2014.

[IF-IMC] Trusted Computing Group, "TCG Trusted Network Connect TNC IF-IMC, Version 1.3", February 2013.

[IF-IMV] Trusted Computing Group, "TCG Trusted Network Connect TNC IF-IMV, Version 1.4", December 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5792] Sangster, P. and K. Narayan, "PA-TNC: A Posture Attribute (PA) Protocol Compatible with Trusted Network Connect (TNC)", RFC 5792, DOI 10.17487/RFC5792, March 2010, <https://www.rfc-editor.org/info/rfc5792>.

[RFC5793] Sahita, R., Hanna, S., Hurst, R., and K. Narayan, "PB-TNC: A Posture Broker (PB) Protocol Compatible with Trusted Network Connect (TNC)", RFC 5793, DOI 10.17487/RFC5793, March 2010, <https://www.rfc-editor.org/info/rfc5793>.

[RFC6876] Sangster, P., Cam-Winget, N., and J. Salowey, "A Posture Transport Protocol over TLS (PT-TLS)", RFC 6876, DOI 10.17487/RFC6876, February 2013, <https://www.rfc-editor.org/info/rfc6876>.

[RFC7632] Waltermire, D. and D. Harrington, "Endpoint Security Posture Assessment: Enterprise Use Cases", RFC 7632, DOI 10.17487/RFC7632, September 2015, <https://www.rfc-editor.org/info/rfc7632>.

[Server-Discovery] Trusted Computing Group, "DRAFT: TCG Trusted Network Connect PDP Discovery and Validation, Version 1.0", October 2015.

[SWID] "Information technology--Software asset management--Part 2: Software identification tag", ISO/IEC 9899:1999, 2009.

Authors' Addresses

Danny Haynes
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
USA

Email: dhaynes@mitre.org

Jessica Fitzgerald-McKay
Department of Defense
9800 Savage Road
Ft. Meade, Maryland
USA

Email: jmfitz2@nsa.gov

Lisa Lorenzin
Pulse Secure
2700 Zanker Rd., Suite 200
San Jose, CA 95134
US

Email: llorenzin@pulsesecure.net